

XceedID™ Application Note #4 (Preliminary – revised 08/22/05)

XceedID Secure *ISO* X Readers and Cards

PURPOSE

The purpose of this Application Note is to provide information about the capabilities of XceedID Corporation's patent pending ISO X™ technology and products. This document will specifically focus on XceedID's ISO X secure ISO 15693/14443 implementation.

INTRODUCTION

The name ISO X (pronounced ISO X) demonstrates that these products are flexible and capable of meeting virtually any contactless ISO standard including the most popular contactless 13.56 MHz RF standards, ISO14443 and ISO15693. ISO X readers are also capable of reading older more established (and less secure) 125 kHz proximity technologies. Because these readers function across various frequencies they are referred to as multi-technology readers. One of the main reasons XceedID offers multi-technology readers is to provide a migration or transition path from old technology to new technology with the same reader device.

ISO X readers and cards from XceedID have been designed to be compatible with existing security access control systems.

The product platform is based on Infineon Technologies secure my-d® IC technology as well as Philips Electronics secure MIFARE® IC Technology. This platform is intended for high security applications. The flexibility provided by the product line is well suited for multiple applications to reside on the same card or credential. Examples of possible applications include Biometrics, Cashless Vending and Payment, Logical Access, Time & Attendance, Medical Records, Personal Information, etc.

XceedID ISO X readers communicate by 13.56 MHz RF and 125 kHz RF energy. Today, XceedID provides passive credentials which mean the credentials (cards) have no battery and therefore receive power to communicate from the reader's RF energy. ISO X readers have been designed to be compatible with industry leading MIFARE technology (card serial number reads) and future updates (Q3 '05) to ISO X readers will include secure MIFARE and secure DESFire implementations. Presently, ISO X readers have been designed to offer an enhanced secure 15693/14443 alternative to HID Corporation's iCLASS® products. When compared to iCLASS, XceedID ISO X readers should demonstrate more flexibility due to multi-technology, better read range performance, and enhanced security.

ISO STANDARDS

ISO X readers are compatible with contactless standards 14443 and 15693. These standards were developed through collaboration by industry leading silicon providers (Philips, Infineon, TI, ST

Microelectronics, etc) with the International Standards Organization (ISO). Two of the most distinguishing factors between the standards are the maximum data rate provided and the typical or maximum read range provided. The U.S. government recently settled on ISO14443 for its standard mainly because of anticipated data intensive applications requiring high data rates. For data intense applications such as multiple biometric templates, ISO 14443 is a logical choice. However, for applications that may involve limited biometrics and where greater read ranges are desired, ISO 15693 is the easy choice. XceedID has developed its ISO[✕] secure implementation to combine the benefits of ISO 15693 and ISO 14443 under the same security scheme and memory map. As an example, a given facility may require that most personnel carry 10K bit credentials, perhaps with a fingerprint biometric template on the card. A smaller percentage of the personnel may require a larger 20K bit credential for multiple templates and other large applications. In this example, the 10K bit card is a 15693 credential while the 20K bit card is 14443 compliant. The larger card takes advantage of the higher data rate to process more information quickly. The reader automatically knows whether it should process a 15693, 14443 or even standard 125 kHz proximity card.

XceedID ISO[✕] READERS

As of this writing there are three ISO[✕] contactless reader models:

- **XF1100** – mullion reader typically used on storefront or narrow stile doorframes
- **XF2100** – mid range reader mounts on US junction boxes (single gang)
- **XF2110** – mid range reader with keypad, mounts on US junction boxes (single gang)

All readers provide a wiegand output. Other reader models are also capable of providing serial RS485 communications (custom protocol by user – contact factory for details).

ISO[✕] readers have been optimized to provide exceptional read range across multiple frequencies and technologies. The readers are offered in two standard colors: black and charcoal gray (custom colors are available). The readers are capable of outputting data in multiple wiegand formats (custom formats are available).

The standard reader configuration is a RED LED on until a credential is presented. A valid read is indicated with a GREEN LED and a “Beep”. Readers are also available with configuration options.

SECURE CREDENTIALS

XceedID secure ISO[✕] credentials are programmed at XceedID’s factory. Standard credential types include clamshell cards (part no. 9440), ISO style cards (part no. 9540) and keytags (“fobs”) (part no. 9640). Secure communication is explained in the security section of this document.

Since XceedID readers function with multiple ISO standards, ISO~~X~~ readers will read the UID of the following 13.56 MHz credentials:

HID iCLASS®

- Inside Contactless PicoTag® and PicoPass®
- Infineon my-d® (“P” plain cards only)
- Philips MIFARE® (S50 – 1K, S70 – 4K, Mifare Pro IC, Mifare Lite)
- Philips MIFARE DESFire®
- ST Microelectronics 15693
- Texas Instruments Tag-it® 15693

The ISO~~X~~ readers are capable of reading secure credentials from one or more technologies and UID’s from multiple other technologies. However, by default, the reader is configured to read ISO~~X~~ 2S and 10S secure credentials (part no. 9532 and 9540 ISO cards). In this mode, it will not report UID’s from 2S and 10S secure credentials for obvious security reasons.

Standard data output for Mifare is 32 bit. Standard 15693 UID data output is 40 bit. Custom outputs are available.

Secure credentials are available in the following memory sizes: 2K bits (“2S”), 10K bits (1.25K bytes referred to as “10S”), or 20K bits (2.5K bytes, referred to as “20S”). The memory maps for the various card styles are shown in the security section of this document. Secure MIFARE and DESFire credentials will be available and implemented in Q4 ’05.

*When using the 20S secure credential the reader must be **specialy configured** and*

will no longer read UID’s or serial numbers for ISO14443 (Mifare, etc.).

HARDWARE

ISO~~X~~ readers are furnished with a 12 conductor, 22AWG 18” pigtail. The wire color chart below, also provided in each reader’s installation manual, provides the wiring instructions:

Yellow	Beeper
Blue	Hold
Purple	Future
Green	Data 0
White	Data 1
Orange	Green LED
Brown	Red LED
Red	Power + DC (8-16VDC)
Black	Ground
Pink	REX (Request to Exit)
Gray	DI (Door Input)
Tan	Tamper Output (External)
Drain	Shield Ground

Use a DC power source between 8-16 volts. Verify the reader is properly grounded by attaching the ground wire to an earth ground connection at the power supply or panel end of the cable. Maximum current requirements are as follows: 125 mA DC Average, 200 mA DC Peak.

ISO~~X~~ readers are equipped with a unique tamper scheme which detects presence and configuration of the reader cover. If the cover is removed an audible alarm is triggered. In addition, the tamper output will remain in a logic low state until the tamper condition is removed.

XceedID(TM), XACTT(TM) and ISO-X(TM) are trademarks of XceedID Corporation. GE®, CASI® and ProxLite® are registered trademarks of General Electric Corporation. MIFARE®, I-Code® and DESFire® are registered trademarks of Philips Electronics, Inc. HID® and iCLASS® are registered trademarks of HID Corporation. my-d® and Infineon® are registered trademarks of Infineon. Other product names mentioned herein may be trademarks and / or registered trademarks of other companies.

XceedID ISO[✕] readers have the following certifications: FCC, CE Mark, Canadian Certification, UL294 Listed, R&TTE Directive – 15 EU Countries

ISO[✕] Credentials

XceedID offers two standard sizes of secure read/write credentials, the 2S (clamshell is part # 9432) and the 10S (clamshell is part # 9440 and ISO is 9540). Both the 2S and the 10S are secure ISO15693 compliant read/write memory IC's. The 10S is well suited for traditional access control environments, providing solid read range and enough memory to handle additional applications including most biometrics.

The custom ordered 20S (ISO card is part no. 9546) is a secure ISO14443 compliant read/write memory IC. The 20S is best used where large data intensive applications, and possibly multiple biometrics will be employed. Since the 20S is 14443 compliant it can take advantage of higher allowable data rates allowing it to handle large transactions more quickly than 15693 compliant IC's such as the 10S. This means a large biometric template can be transferred and authorized or denied much more quickly and seamlessly between the card and the reader. *As a reminder, all readers must be custom configured to read the 20S securely. In reading the 20S securely the reader will no longer read UID's or serial numbers from other ISO 14443 credentials.*

Memory Organization

The following tables describe the memory map for the ISO[✕] credentials (2S, 10S, and 20S). The memory is divided into 128 pages for the 10S or 256 pages for the 20S (only 31 pages for the 2S). Each page consists of 10 bytes: 8 bytes of data and 2 bytes to define the access right and application index. The memory is divided into three major memory areas. The following example is for the 10S:

- **The administration area** (pages 0 thru 13): consists of the UID, issuer data, the administration pages and the authentication keys.
- **The access control application area** (pages 14 thru 19): consists of access control information to be sent to the access control system panel, passwords, keypad PINs, etc...
- **The area reserved for other applications** (pages 20 thru 127 or 255): This could be employee data, a cashless vending application, time&attendance, medical records, etc.

These maps are standard maps defined for a variety of applications. **Custom maps are also available on demand.** For example the number of applications could be increased or reduced and the memory could be tailored for specific applications (vending, parking, etc). The maximum allowable number of application areas is 14 (including the Access Control application).

Figure 1 – Memory map for the ISO ~~X~~ 2S

Page	Data
31	Application 4 [16 bytes]
30	
29	Application 3 [24 bytes]
28	
27	
26	Application 2 Debit / Credit [24 bytes]
25	
24	
23	Application 1 [32 bytes]
...	
20	
19	Access Control Application
...	
14	
13	Application 4 KeyB
12	Application 4 KeyA
11	Application 3 KeyB
10	Application 3 KeyA
9	Application 2 KeyB
8	Application 2 KeyA
7	Application 1 KeyB
6	Application 1 KeyA
5	Access Control Application KeyB
4	Access Control Application KeyA
3	Authentication Counter
2	AFI AC Manufacturer Code
1	IT AN Issuer Data
00	Unique Identification Number

Figure 2 – Memory map for the ISO ~~X~~ 10S

Page	Data
127	Application 4 Large Template Area [784 bytes]
...	
30	
29	Application 3 [24 bytes]
28	
27	
26	Application 2 Debit / Credit [24 bytes]
25	
24	
23	Application 1 [32 bytes]
...	
20	
19	Access Control Application
...	
14	
13	Application 4 KeyB
12	Application 4 KeyA
11	Application 3 KeyB
10	Application 3 KeyA
9	Application 2 KeyB
8	Application 2 KeyA
7	Application 1 KeyB
6	Application 1 KeyA
5	Access Control Application KeyB
4	Access Control Application KeyA
3	Authentication Counter
2	AFI AC Manufacturer Code
1	IT AN Issuer Data
00	Unique Identification Number

Figure 3 – Memory map for the ISO^X 20S

Page	Data
255	Application 5
...	Open area (no security)
238	[144 bytes]
237	Application 4
...	Large Template Area [1664 bytes]
30	
29	Application 3
28	[24 bytes]
27	Application 2
26	Debit / Credit [24 bytes]
25	Application 1
24	[32 bytes]
23	Application 1
...	[32 bytes]
20	
19	Access Control Application
...	
14	
13	Application 4 KeyB
12	Application 4 KeyA
11	Application 3 KeyB
10	Application 3 KeyA
9	Application 2 KeyB
8	Application 2 KeyA
7	Application 1 KeyB
6	Application 1 KeyA
5	Access Control Application KeyB
4	Access Control Application KeyA
3	Authentication Counter
2	AFI AC Manufacturer Code
1	IT AN Issuer Data
0	Unique Identification Number

The table below (Figure 4) denotes the card memory size and available memory space for applications. The Access Control application area is not included in these numbers. Both credentials allow the storage of significantly large or multiple biometric templates as well as various other applications.

	Card memory size	Available memory space for other applications
ISO ^X 2S	2560 bits (320 bytes)	96 bytes (pages 20 to 31)
ISO ^X 10S	10240 bits (1280 bytes)	864 bytes (pages 20 to 127)
ISO ^X 20S	20480 bits (2560 bytes)	1888 bytes (pages 20 to 255)

Figure 4 – Available data memory for the ISO^X credentials

XceedID Security

The XceedID smart card system offers a high level of security and data integrity through the judicious use of the cryptographic techniques described below.

Mutual Authentication

The memory of the ISO^X credential is divided into several sectors also called applications. Each sector is secured by an *Authentication key*. A reader can only access a secure sector after a successful mutual authentication is performed. The mutual authentication can only be successful if the reader and the card share a common secret: the mutual authentication key.

The ISO^X authentication process never transmits the authentication key. Instead, it creates digital signatures derived from random numbers created by the reader and the credential and the credential UID (unique ID) making each communication session different, unique and authentic. A successful mutual authentication allows the reader and credential to securely authenticate each other, eliminating the risk of unauthorized communication transactions between the card and the reader.

Message Authentication Codes

After a successful authentication has taken place between the reader and the credential, the communication between these two devices is authorized and the reader has access to the authenticated sector or

application. Each message going back and forth between the reader and the credential is digitally signed, ensuring that the communication remains authentic at all times and that an unauthorized device cannot interfere with the communication between the credential and the reader.

In summary, all communication following the mutual authentication is also secure. The use of digital signatures or Message Authentication Codes (MACs) ensures that every piece of information traveling between the card and the reader is authentic. The ISO^X smart card system is the only ISO-15693 access control system offering Message Authentication Coding.

Keys and Key Diversification

The size of the mutual authentication key employed by the ISO^X Smart Card system is 128 bits (this key is called the *System Key* and resides in the reader). Each ISO^X 10S credential has a unique 64-bit ID (UID) as defined in ISO 15693. Each ISO^X 20S credential has a 56 bit UID as defined in ISO 14443. The ISO^X system takes advantage of this feature to derive a unique 64-bit key for each credential (this is called a *Card Key* because it resides in the card).

This process is called key diversification and provides strong protection of the system key. In effect, even if a card key is known, it cannot be maliciously used to attack the system and cannot be employed to duplicate a credential because the system key cannot be deduced from card keys.

Data Encryption

The ISO^X smart card system offers encryption of the data stored on the credential. The credential memory organization is based on a 64-bit page structure. The encryption algorithms employed by the ISO^X system are the popular DES and 3DES, which are strong algorithms. These algorithms are well suited for the ISO^X memory organization.

Encryption is optional and only provides added privacy. Most access control data does not consist of private information, making encryption unnecessary in most cases. However, if applications contain private information such as the user's social security numbers, encryption is highly recommended.

ISO^X Security Benefits		
	Purpose	Key description
Mutual Authentication	Authentication between credential and reader. Opens access to memory sector of the credential. Reader can read/write to memory sector	128-bit System key. 64-bit card keys: 2 keys with different privileges protect each sector. For example, one card key could allow read access only, while the other could allow read/write
Message Authentication Codes	Maintains authenticity of the RF communication from beginning to end, increasing security and providing data integrity	Based on the original 64-bit card keys and authentication procedure. MACs are different for every transaction and cannot be duplicated
Key Diversification	Protects the 128-bit system key by creating 64-bit keys unique to each credential using the UID of the credential. The system key is never transmitted from the reader to the credential (not even during the credential programming phase)	<ul style="list-style-type: none"> - 128-bit system key resides in the reader. It cannot be read and is never transmitted. - 64-bit card key resides in the card. It is derived from the card UID and the system key using a key diversification algorithm. The key is never transmitted by the card. It cannot be read.
Encryption	Encryption of the card data provides confidentiality. Encryption is optional	<ul style="list-style-type: none"> - 56-bit key if using DES - 112-bit key if using 3DES

Key Management

Keys are large numbers that are kept secret to protect a security system. They are chosen from a vast number of values also called “keyspace”. These numbers are so large that it is impossible to guess their value. The following table is helpful in understanding the magnitude and significance of these large numbers.

Large Numbers	
Possible combinations on a typical door lock	Less than 20,000
Possible combinations for a US state lottery	1 Million
Planets in our known universe	1 Trillion
Possible authentication keys in the XceedID 64-bit keyspace	Over 18 Billion Trillions*

*= this is the actual number of possibilities: 18,446,744,073,709,551,616

A successful authentication between the card and the reader is possible if:

- The card knows the key
- The reader knows the key

The ISO^X access control application is protected by an authentication key that must be programmed into readers and cards.

ISO^X standard key: if a custom key is not specified, all readers will be programmed with the same standard system key and every card will be programmed with a unique key derived from the standard system key. The system key is never transmitted and is kept securely in the reader. Any system of cards and readers configured with the standard key are compatible with one another and the access control application will be executed seamlessly (so long as the access control system is programmed to allow access to the specific credential).

ISO^X custom key: The standard key can be replaced with a custom key. Cards and readers must be programmed with this new key. XceedID will generate and distribute custom keys. XceedID will program cards and readers with the custom key. XceedID will also provide tools to upload custom keys into readers already deployed. A custom key provides an additional layer of security, because a custom key system will not communicate with credentials outside of the custom key system, making the access control application custom as well.